appeal within thirty days of receiving the defendant's appeal and supporting brief.

(g) If a defendant timely files a notice of appeal, and the time for filing reconsideration motions has expired, the ALJ will forward the record of the proceeding to the authority head.

(h) An initial decision is automatically stayed pending disposition of a motion for reconsideration or of an appeal to the authority head.

(i) No administrative stay is available following the authority head's final decision.

§ 1174.38 Appeal to the authority head.

(a) A defendant has no right to appear personally, or through a representative, before the authority head.

(b) There is no right to appeal any interlocutory ruling.

(c) The authority head will not consider any objection or evidence that was not raised before the ALJ unless the defendant demonstrates that extraordinary circumstances excuse the failure to object. If the defendant demonstrates to the authority head's satisfaction that extraordinary circumstances prevented the presentation of evidence at the hearing, and that the additional evidence is material, the authority head may remand the matter to the ALJ for consideration of the additional evidence.

(d) The authority head may affirm, reduce, reverse, compromise, remand, or settle any penalty or assessment that the ALJ imposed in the initial decision or reconsideration decision.

(e) The authority head will promptly serve each party to the appeal and the ALJ with a copy of the decision. This decision must contain a statement describing the right of any person, against whom a penalty or assessment has been made, to seek judicial review.

§ 1174.39 Judicial review.

31 U.S.C. 3805 authorizes the appropriate United States District Court to review any final decision imposing penalties or assessments, and specifies the procedures for such review. To obtain judicial review, a defendant must file a petition with the appropriate court in a timely manner.

§ 1174.40 Collection of civil penalties and assessments.

31 U.S.C. 3806 and 3808(b) authorize actions for collecting civil penalties and assessments imposed under this part and specify the procedures for such actions.

§ 1174.41 Rights to administrative offset.

The authority may make an administrative offset under 31 U.S.C. 3716 to collect the amount of any penalty or assessment which has become final, for which a judgment has been entered, or which the parties agree upon in a compromise or settlement. However, the authority may not make an administrative offset under this subsection against a Federal tax refund that the United States owes to the defendant then or at a later time.

§ 1174.42 Deposit in Treasury of the United States.

The authority shall deposit all amounts collected pursuant to this part as miscellaneous receipts in the Treasury of the United States, except as provided in 31 U.S.C. 3806(g).

§ 1174.43 Voluntary settlement of the administrative complaint.

(a) Parties may make offers of compromise or settlement at any time. Any compromise or settlement must be in writing.

(b) The reviewing official has the exclusive authority to compromise or settle the case from the date on which the reviewing official is permitted to issue a complaint until the ALJ issues an initial decision.

(c) The authority head has exclusive authority to compromise or settle the case from the date of the ALJ's initial decision until initiation of any judicial review or any action to collect the penalties and assessments.

(d) The Attorney General has exclusive authority to compromise or settle the case while any judicial review or any action to recover penalties and assessments is pending.

(e) The investigating official may recommend settlement terms to the reviewing official, the authority head, or the Attorney General, as appropriate.

§ 1174.44 Limitations regarding criminal misconduct.

(a) Any investigating official may:

(1) Refer allegations of criminal misconduct or a violation of the False Claims Act directly to the Department of Justice for prosecution and/or civil action, as appropriate;

(2) Defer or postpone a report or referral to the reviewing official to avoid interference with a criminal investigation or prosecution; or

(3) Issue subpoenas under any other statutory authority.

(b) Nothing in this part limits the requirement that the authority's employees must report suspected violations of criminal law to the NEH Office of the Inspector General or to the Attorney General.

Dated: August 2, 2021.

Elizabeth Voyatzis,

Deputy General Counsel, National Endowment for the Humanities.

[FR Doc. 2021–16763 Filed 8–12–21; 8:45 am]

BILLING CODE 7536–01–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 20

[GN Docket No. 13–111; FCC 21–82; FR ID 39494]

Promoting Technological Solutions To Combat Contraband Wireless Device Use in Correctional Facilities

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission or FCC) takes further steps to facilitate the deployment and viability of technological solutions used to combat contraband wireless devices in correctional facilities. The *Second Report and Order* adopts a framework requiring the disabling of contraband wireless devices detected in correctional facilities upon satisfaction of certain criteria, and we address issues involving oversight, wireless provider liability, and treatment of 911 calls. The *Second Report and Order* further adopts rules requiring advance notice of certain wireless provider network changes to promote and maintain contraband interdiction system effectiveness.

DATES: This final rule is effective September 13, 2021, with the exception of the revisions to § 20.23, which are delayed. The Commission will publish a document in the **Federal Register** announcing the effective date for those revisions.

FOR FURTHER INFORMATION CONTACT: Melissa Conway of the Wireless Telecommunications Bureau, Mobility Division, at (202) 418–2887 or *Melissa.Conway@fcc.gov.* For information regarding the Paperwork Reduction Act of 1995 (PRA) information collection requirements contained in this document, contact Cathy Williams, Office of Managing Director, at (202) 418–2918 or *Cathy.Williams@fcc.gov.*

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *Second Report and Order* in GN Docket No. 13–111, FCC 21–82 adopted July 12, 2021 and released July 13, 2020. The full text of the *Second Report and Order,* including all Appendices, is available

for inspection and copying during normal business hours in the FCC Reference Center, 45 L Street NE, Washington, DC 20554, or available for viewing via the Commission's ECFS website by entering the docket number, GN Docket No. 13–111. Alternative formats are available for people with disabilities (Braille, large print, electronic files, audio format), by sending an email to *FCC504@fcc.gov* or calling the Consumer and Governmental Affairs Bureau at (202) 418–0530 (voice), (202) 418–0432 (TTY).

The Commission will send a copy of this *Second Report and Order* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. 801(a)(1)(A).

Final Regulatory Flexibility Analysis

The Regulatory Flexibility Act (RFA) requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that ''the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities.'' Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this *Second Report and Order* on small entities. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Further Notice of Proposed Rulemaking* (*FNPRM*) released in March 2017 in this proceeding (82 FR 22780, May 18, 2017). The Commission sought written public comment on the proposals in the *FNPRM,* including comments on the IRFA. No comments were filed addressing the IRFA. This present Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.

Paperwork Reduction Act

The requirements in § 20.23(b) through (d) include new or modified collections subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104–13. They will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding. In addition, the Commission notes that, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4), the Commission previously sought, but did not receive, specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees. The Commission describes impacts that might affect small businesses, which includes more businesses with fewer than 25 employees, in the Final Regulatory Flexibility Analysis.

Congressional Review Act

The Commission will send a copy of this *Second Report and Order* to Congress and the Government Accountability Office pursuant to the Congressional Review Act. *See* 5 U.S.C. 801(a)(1)(A). In addition, the Commission will send a copy of the *Second Report and Order,* including this FRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). A copy of the *Second Report and Order,* and FRFA (or summaries thereof) will also be published in the **Federal Register**.

Synopsis

1. The *Second Report and Order* adopts new or additional reporting or recordkeeping and compliance obligations for small entities as well as other applicants and licensees. Small entities may have to hire attorneys, engineers, consultants, or other professionals in order to meet the reporting, recordkeeping or compliance obligations in the *Second Report and Order,* however, the Commission cannot quantify the cost of compliance with the requirements. To minimize burdens, we have adopted processes and procedures where possible to allow direct interaction between the Designated Correctional Facility Officials (DCFOs) and the wireless providers and avoided interjecting the Commission and additional regulations into the process. In our approach, we sought to provide small and other entities flexible options such as giving DCFOs and wireless providers the flexibility to structure the format of the qualifying requests in a way that meets the unique needs of the parties rather than adopting a standardized form. We also adopted minimum requirements for information to be included in a qualifying request to disable a contraband device and allowed for self-certification to meet the certification requirements. Below we discuss reporting, recordkeeping, and/or compliance requirements adopted in the *Second Report and Order.*

2. *Designated Correctional Facility Official Requirements.* The *Second Report and Order* requires that a DCFO satisfy certain requirements in order to submit qualifying requests to wireless providers. Specifically, qualifying disabling requests must be submitted by a DCFO, which we define as an official of the state, local, or Federal government with responsibility for oversight of the relevant facility. In government-run correctional facilities, this definition requires the DCFO to be, at a minimum, the official with responsibility for oversight of the relevant facility (*e.g.,* the warden) or higher ranking official; in privately-run correctional facilities, the DCFO must be a government official with responsibility for oversight of the facility's performance through a contract.

3. The *Second Report and Order* also adopts a process for certification of DCFOs that will provide certainty to wireless providers that disabling requests are duly authorized by the relevant Federal, state, or local government entities. The Commission will maintain a publicly available list of DCFOs that are authorized to transmit qualifying disabling requests. Authorized individuals that wish to be recognized on the Commission's DCFO list must send a letter to the Commission's Contraband Ombudsperson, signed by the relevant state attorney general, providing the individual's name, official government position, and a list of correctional facilities over which the individual has oversight and management authority.

4. *Authorization of CISs.* The *Second Report and Order* establishes a two-phase authorization process for Contraband Interdiction System (CIS) applicants seeking to deploy CISs that will provide the requisite information necessary for DCFOs to submit qualifying requests to disable contraband devices at qualifying correctional facilities. In phase one, CIS applicants will submit applications to the Wireless Telecommunications Bureau (the Bureau) describing their legal and technical qualifications of the systems. The Bureau will review the applications and approve—at a system level—those CISs that meet the requirements. In phase two, CIS applicants will perform on-site testing of approved CISs at individual qualifying correctional facilities. After both phases are complete, DCFOs will be authorized to submit qualifying requests to disable contraband devices using approved CISs at each approved correctional facility.

5. *CIS Certification Process.* The *Second Report and Order* adopts a CIS certification process for detection systems to be used in qualifying requests. To obtain CIS certification, a CIS applicant must submit an application to the Bureau for review and

approval. The application must demonstrate, at a minimum that: (1) All radio transmitters used as part of the CIS have appropriate equipment authorization pursuant to Commission rules; (2) the CIS is designed and will be configured to locate devices solely within a correctional facility; (3) the methodology to be used in analyzing data collected by the CIS is sufficiently robust to ensure that the particular wireless device is in fact located within a correctional facility, including specific data analysis benchmarks designed to ensure successful detection, such as rate of detection of contraband versus non-contraband devices, relevant sample size (*e.g.* number of devices observed and length of observation period); (4) the CIS will secure and protect all information or data collected as part of its intended use; and (5) the CIS will not interfere with emergency 911 calls. The application must also include a description of whether the CIS requires a spectrum or network access agreement (*e.g.,* a spectrum leasing arrangement and/or roaming agreement) to be authorized to operate. Finally, the application must include a proposed test plan for subsequent site-based testing of each CIS, which must include detailed descriptions and technical specifications to facilitate Commission review of whether the system satisfies its legal requirements and technically functions as anticipated.

6. *Site-Based Testing and Self-Certification Requirement.* In the second phase of the CIS authorization process, a CIS operator—which could be a CIS solutions provider, or a DCFO or other responsible party that deploys its own CIS at a correctional facility [1]—seeking to use the CIS to submit qualifying requests for disabling contraband devices must test a certified CIS at each location and, thereafter, must file a self-certification to the Bureau confirming that the testing at that specific correctional facility is complete and successful. The CIS operator must also serve notice of the testing on each of the wireless providers holding a spectrum license that includes the county within which the correctional facility is located and provide a reasonable opportunity to participate in the tests. Following the testing, and to be eligible for use in conjunction with qualifying requests for disabling, the CIS operator must submit a self-certification that: (1) Identifies the correctional facility where it seeks to deploy; (2) attests that applicable federal or state criminal statutes prohibit possession or operation of contraband devices within the correctional facility (and includes the applicable federal or state criminal statutory provision); (3) describes the results of on-site tests of the certified CIS conducted at the correctional facility; (4) attests that the on-site testing was performed consistent with the approved test plans for the certified CIS and that the CIS deployment minimizes the risk of disabling a non-contraband device; (5) identifies whether any wireless providers participated in the testing, and provides proof that the wireless providers were given notice regarding the testing and a reasonable opportunity to participate; and (6) includes proof of any spectrum and/or network access agreement (*e.g.,* a spectrum leasing arrangement and/or roaming agreement) required to be authorized to operate and/or for the system to function effectively. The self-certification submitted by a CIS operator must be accompanied by an attestation from the DCFO verifying that all information contained in the self-certification is true and accurate.

7. CIS operators must submit self-certifications in accordance with filing procedures established by the Bureau and those certifications must also be served via electronic means on all wireless providers licensed in the geographic area occupied by the correctional facility. Wireless providers have five business days from the certification filing date to submit objections to the Bureau and to serve any such objections on the DCFO and the CIS operator. Absent objections, the DCFO may submit qualifying requests to wireless providers beginning on the sixth business day after the certification filing. If an objection is submitted, the DCFO may not submit qualifying requests until the Bureau addresses the objection.

8. *Records Maintenance.* To ensure the integrity and proper operation of CIS, we require CIS operators to retain records of all information supporting each request for disabling and the basis for disabling each device, for at least five years following the relevant disabling request. CIS operators of systems that have been tested and approved for use in qualifying requests must also make available all records upon request from the Bureau.

9. *Recertification.* In order to ensure the ongoing accuracy and reliability of a given CIS at a particular facility, at least every three years after the initial self-certification, CIS operators seeking to maintain the ability to submit qualifying requests through a DCFO to disable contraband devices must retest their systems and recertify them for continued CIS accuracy. Recertifications must comply with the same rules and filing instructions that apply to the initial self-certification.

10. *Qualifying Requests.* We required that qualifying requests to disable a contraband device include the following material: (1) A certification that (a) A certified CIS was used to gather the contraband subscriber and device information populated in the qualifying request; (b) the certified CIS was used to identify contraband devices operating in a correctional facility where the CIS has been tested and self-certified for operational readiness and for use in qualifying requests, and the identification of contraband devices occurred within 30 days immediately prior to the date of the qualifying request submission; (c) the DCFO has reviewed the list of contraband devices and attests that it is accurate; and (d) it is a violation of applicable state or federal criminal statutes to possess or operate a contraband device in the correctional facility; (2) the name and address of each requesting correctional facility; and (3) a list of contraband devices with identifiers sufficient to uniquely describe the devices in question at both the subscription and device level.

11. *Disabling Process and Timeframe for Disabling a Contraband Device.* The *Second Report and Order* adopts the following process for disabling contraband devices. Upon receipt of a qualifying request from a DCFO through a verifiable and secure transmission method, a wireless provider must treat the request as valid. The wireless provider may only reject a request if the request fails to meet the Commission-mandated information for a qualifying request or if there are errors with respect to the device identifying information that leave the wireless provider unable to disable the device. Unless a wireless provider finds these grounds to reject the qualifying request, it must, within two business days after receipt of a qualifying request: (1) Disable the device at both the subscriber level and at the device level; and (2) take reasonable and practical steps to prevent an identified device from being accessing another wireless provider's network (*e.g.,* by adding the equipment identifier to the Stolen Phone Database). A wireless provider must inform the DCFO whether or not the request has been granted within two business days of receiving the qualifying request.

12. *Reversals.* A wireless provider may subsequently reverse a device disabling if it determines that the device was identified erroneously as

[1] *See* Appendix A, Final Rules, of the Second Report and Order (adding definition to § 20.3 of the Commission's rules, 47 CFR 20.3).

contraband. If the wireless provider chooses to reverse a disabling, however, it must promptly inform the DCFO of the mistakenly identified device. The *Second Report and Order* also provides wireless providers with the option to trigger the involvement of the DCFO in the reviewing the validity of a device previously identified and disabled as contraband. If the wireless provider seeks to trigger the DCFO's involvement, it must provide the DCFO with: (1) The date of the qualifying request, (2) the identifying information provided for the device, and (3) any evidence supporting the wireless provider's belief that the device was erroneously identified. The *Second Report and Order* states that, upon receipt of such a request, the DCFO should review the qualifying request to determine whether the device in question was erroneously identified and either: (1) Confirm the validity of the identifying information contained in the qualifying request, or (2) acknowledge the error and direct the carrier to restore service to the device. In the event the DCFO directs the wireless provider to reverse the disabling, the wireless provider must, within two business days, restore service to the device and reverse any actions taken to prevent the device from accessing other wireless provider networks (*e.g.,* by removing the phone from the Stolen Phone Database). In the event the DCFO does not respond to a request from a wireless provider for review of a qualifying request within two business days, the wireless provider may proceed with reversing the disabling action. The *Second Report and Order* requires the DCFO to provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices on a quarterly basis at the end of any quarter during which a device disabling was reversed, and directs the Wireless Telecommunications Bureau to issue a public notice providing additional guidance regarding the appropriate method for providing such notice.

13. *Transmission of the Qualifying Request.* DCFOs must transmit a qualifying request to a wireless provider using a verifiable and secure transmission method, and a wireless provider must adopt a method, or utilize an existing method, for receiving secured and verified qualifying requests. The *Second Report and Order* directs the Contraband Ombudsperson to work with wireless providers to develop suitable methods for securely transmitting a qualifying request.

14. *Notification to CIS Operators of Wireless Provider Technical Changes.* Commercial Mobile Radio Service (CMRS) licensees leasing spectrum to managed access systems (MAS) must provide 90 days advance notice to MAS operators of the following network changes occurring within 15 miles of the correctional facility, while permitting modified notice arrangements through mutual agreement: (1) Adding a new frequency band to service offerings; (2) deploying a new air interface technology or changing an existing air interface technology; and/or (3) adding, relocating, or removing a site. This limited notification requirement is necessary to deploy MAS effectively. The *Second Report and Order* adopts an exception to the 90-day advance notice requirement for network technical changes within 15 miles of the facility that are required due to emergency/disaster preparedness, but it requires CMRS licensees to provide notice of these technical changes immediately after the exigency. The *Second Report and Order* also requires CMRS licensee lessors and MAS operator lessees to negotiate in good faith to reach an agreement for notification for other, more localized types of network adjustments not covered bv the major network change notice requirement. The *Second Report and Order* further requires CMRS licensees and MAS operators to negotiate in good faith regarding the parties' treatment of confidential information contained in notifications required by rule and/or negotiated between the parties.

List of Subjects in 47 CFR Part 20

Administrative practice and procedure, Common carriers, Communications, Communications common carriers, Communications equipment, Environmental impact statements, Radio, Reporting and recordkeeping requirements, Satellites, Security measures, Telecommunications, Telephone.

Federal Communications Commission.

Cecilia Sigmund,

Federal Register Liaison Officer, Office of the Secretary.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR part 20 as follows:

PART 20—COMMERCIAL MOBILE SERVICES

■ 1. The authority citation for part 20 continues to read as follows:

Authority: 47 U.S.C. 151, 152(a), 154(i), 155, 157, 160, 201, 214, 222, 251(e), 301, 302, 303, 303(b), 303(r), 307, 307(a), 309, 309(j)(3), 316, 316(a), 332, 610, 615, 615a, 615b, and 615c, unless otherwise noted.

■ 2. Amend § 20.3 by adding the definitions of ''CIS Operator,'' ''Contraband Interdiction System,'' ''Designated Correctional Facility Official,'' ''Managed Access System'' in alphabetical order to read as follows:

§ 20.3 Definitions.

* * * * *

CIS Operator. An operator of a CIS at a correctional facility, whether a CIS solutions provider, or a DCFO or responsible party that deploys its own CIS at a correctional facility.

* * * * *

Contraband Interdiction System. A Contraband Interdiction System (CIS) is any system comprised of one or more stations that is used only at a permanent correctional facility that is authorized to operate such systems pursuant to this part and that is designed exclusively to prevent transmissions to or from contraband wireless devices within the boundaries of the facility and/or to obtain identifying information from such contraband wireless devices.

Designated Correctional Facility Official. A Designated Correctional Facility Official (DCFO) is an official of the state, local, or Federal government responsible for administration and oversight of the relevant correctional facility where a contraband wireless device is located.

(1) In government-run correctional facilities, this definition requires the DCFO to be, at a minimum, the official with responsibility for oversight of the relevant facility (*e.g.,* the warden) or higher ranking official.

(2) In privately-run correctional facilities, this definition requires the DCFO to be a government official with responsibility for oversight of the facility's performance through contract.

* * * * *

Managed Access System. A Managed Access System (MAS) is a Contraband Interdiction System whose operations require:

(1) One or more lease agreements with CMRS operators; and

(2) Real-time awareness of wireless provider spectrum use in the vicinity of the correctional facility where it is deployed.

* * * * *

■ 3. Delayed indefinitely, amend § 20.23 by adding paragraphs (b) through (d) to read as follows:

§ 20.23 Contraband wireless devices in correctional facilities.

* * * * *

(b) *Contraband Interdiction System (CIS) authorization process.* The

provisions in this section apply to any person seeking certification of a CIS authorized for use in the submission of qualifying disabling requests, whether operating a system that requires a license and is regulated as CMRS or private mobile radio service (PMRS), or operating a passive system that does not require a license. The Wireless Telecommunications Bureau (Bureau) will establish, via public notice, the form and procedure for: CIS operators to file CIS certification applications, self-certifications, and periodic re-certification; CIS operators to serve on wireless providers notice of testing and copies of self-certification; and wireless providers to file objections to self-certifications, including required service on CIS operators and DCFOs.

(1) *Application requirements.* To obtain CIS certification, an applicant must submit an application to the Bureau for review and approval that:

(i) Demonstrates that all radio transmitters used as part of the CIS have appropriate equipment authorizations pursuant to Commission rules in part 2 of this chapter;

(ii) Demonstrates that the CIS is designed and will be configured to locate devices solely within a correctional facility;

(iii) Describes the methodology to be used in analyzing data collected by the CIS and demonstrates that such methodology is adequately robust to ensure that the particular wireless device is in fact located within a correctional facility and includes specific data analysis benchmarks designed to ensure successful detection, such as rate of detection of contraband versus non-contraband devices and relevant sample size (*e.g.* number of devices observed and length of observation period);

(iv) Demonstrates that the CIS will secure and protect all information or data collected as part of its intended use;

(v) Demonstrates that the CIS will not interfere with emergency 911 calls;

(vi) Describes whether the CIS requires a spectrum or network access agreement (*e.g.,* a spectrum leasing arrangement or roaming agreement) to be authorized to operate; and

(vii) Includes a proposed test plan for subsequent site-based testing of each CIS, that must include detailed descriptions and technical specifications to facilitate Commission review of whether the system satisfies its legal requirements and technically functions as anticipated.

(2) *Marketing and sales.* CIS that are certified for use in qualifying requests for disabling of contraband devices may be marketed or sold only to correctional facilities or entities that will provide contraband interdiction services to such facilities.

(3) *Site-based testing and self-certification requirements*—(i) *Site-based testing.* A CIS operator seeking to use the CIS to submit qualifying requests for disabling must test a certified CIS at each location where it intends to operate. Thereafter, the CIS operator must file with the Bureau a self-certification that complies with paragraph (b)(3)(ii) of this section, confirming that the testing at that specific correctional facility is complete and successful. The CIS operator must serve notice of the testing on all relevant wireless providers prior to testing and provide such wireless providers a reasonable opportunity to participate in the tests. Relevant wireless providers include any wireless provider holding a spectrum license that:

(A) Authorizes operation on the frequencies on which the CIS seeks to detect contraband use; and

(B) Authorizes service in the geographic area (*e.g.,* census tract, county, Partial Economic Area (PEA), Economic Area (EA), Cellular Market Area (CMA), Regional Economic Area Grouping (REAG)) within which the correctional facility is located.

(ii) *Self-certification.* Following the testing, and to be eligible for use in conjunction with qualifying requests for disabling, a CIS operator must file a self-certification with the Bureau that:

(A) Identifies the correctional facility where it seeks to deploy;

(B) Attests that applicable Federal or state criminal statutes prohibit the possession or operation of contraband devices within the correctional facility (and includes the applicable Federal or state criminal statutory provision);

(C) Describes the results of on-site tests of the certified CIS conducted at the correctional facility;

(D) Attests that the on-site testing was performed consistent with the approved test plans for the certified CIS and that the CIS deployment minimizes the risk of disabling a non-contraband device;

(E) Identifies whether any relevant wireless providers participated in the testing, and provides proof that the relevant wireless providers were given notice regarding the testing and a reasonable opportunity to participate;

(F) Includes proof of any spectrum and/or network access agreement (*e.g.,* a spectrum leasing arrangement and/or roaming agreement) required to be authorized to operate and/or for the system to function effectively;

(G) Includes proof that the self-certification was served via electronic means on all relevant wireless providers; and

(H) Includes an attestation from the DCFO verifying that all information contained in the self-certification is true and accurate.

(I) The self-certification must be filed in accordance with part 1, subpart F, of this chapter.

(4) *Submitting objections.* Wireless providers may submit objections to the Bureau within five business days from the certification filing date. Any such objections must be served on the DCFO and the CIS operator.

(5) *Recertification.* At least every three years after the initial self-certification, CIS operators seeking to maintain the ability to submit qualifying requests through a DCFO for contraband device disabling must retest their systems and recertify them for continued CIS accuracy. Recertifications must comply with the same rules and filing instructions that apply to the initial self-certification.

(6) *Suspension of CIS eligibility.* The Bureau may suspend CIS certification generally or at a particular facility if subsequent credible information calls into question a system's reliability.

(7) *Records maintenance.* To ensure the integrity and proper operation of CISs, a CIS operator must retain records of all information supporting each request for disabling and the basis for disabling each device, including copies of all documents submitted in the qualifying request, for at least five years following the date of submission of the relevant disabling request. CIS operators of systems that have been tested and approved for use in qualifying requests must make available all records upon request from the Bureau.

(c) *Disabling contraband wireless devices.* A DCFO may request that a CMRS licensee disable a contraband wireless device that has been detected in a correctional facility by a CIS that has been certified in accordance with paragraph (b) of this section. Absent objections from a wireless provider, as described under paragraph (b)(4) of this section, the DCFO may submit a qualifying request to a wireless provider beginning on the sixth business day after the later of the self-certification filing or actual service, as described under paragraph (b)(3)(ii) of this section.

(1) *DCFO list.* The Commission will maintain a publicly available list of DCFOs that are authorized to transmit qualifying disabling requests. Authorized DCFOs that seek to be recognized on the Commission's DCFO list must send a letter to the Commission's Contraband Ombudsperson, signed by the relevant

state attorney general or the relevant Bureau of Prisons Regional Director and providing:

(i) The individual's name;

(ii) The individual's official government position; and

(iii) A list of correctional facilities over which the individual has oversight and management authority.

(2) *Qualifying request.* A qualifying request must be made in writing, contain the certifications in paragraph (c)(2)(i) of this section and the device and correctional facility identifying information in paragraph (c)(2)(ii) of this section, and be signed by the appropriate DCFO. The DCFO must transmit a qualifying request to a CMRS licensee using a secure communication means that will provide certainty regarding the identity of both the sending and receiving parties. A CMRS licensee must adopt a method, or use an existing method, for receiving secured and verified qualifying requests.

(i) *Certifications.* A qualifying request must include the following certifications by the DCFO:

(A) A CIS that has been certified in accordance with paragraph (b) of this section was used to gather the contraband subscriber and device information populated in the qualifying request;

(B) The certified CIS was used to identify contraband wireless devices operating in a correctional facility where the CIS has been tested and self-certified for operational readiness and for use in qualifying requests, and the identification of contraband wireless devices occurred within 30 days immediately prior to the date of the qualifying request submission;

(C) The DCFO has reviewed the list of contraband wireless devices and attests that it is accurate; and

(D) It is a violation of applicable state or Federal criminal statutes to possess or operate a contraband device in the correctional facility.

(ii) *Device and correctional facility identifying information.* The qualifying request must identify the contraband wireless device to be disabled and the correctional facility by providing the following information:

(A) Identifiers sufficient to:

(*1*) Identify the applicable wireless service provider;

(*2*) Uniquely describe each of the contraband wireless devices in question at the subscription level; and

(*3*) Uniquely describe each of the contraband wireless devices in question at the device-level;

(B) Name of the correctional facility at which the contraband wireless device(s) were identified; and

(C) Street address of the correctional facility at which the contraband wireless device(s) were identified.

(3) *Licensee actions upon receipt of a qualifying request.* Upon receiving a request from a DCFO to disable a contraband wireless device, a licensee providing CMRS service must verify that the request contains the required information for a qualifying request, as defined in paragraph (c)(2) of this section.

(i) *Disabling upon receipt of a qualifying request and timing.* If the qualifying request contains the required information, and does not contain an error in the device identifying information preventing the licensee from being able to disable the device, a licensee must, within two business days of receipt of the qualifying request, disable the contraband wireless device from using the wireless provider's network at both the device and subscriber level and take reasonable and practical steps to prevent the contraband wireless device from being used on another wireless provider's network.

(ii) *Rejection of a qualifying request and timing.* A licensee may reject a qualifying request within two business days of receipt of a qualifying request if it does not include the information required for a qualifying request or, with respect to a relevant device, the request contains an error in the device-identifying information preventing the licensee from being able to disable the device.

(iii) *Customer outreach.* A licensee may immediately disable a contraband wireless device without any customer outreach, or a licensee may contact the customer of record through any available means to notify them that the device will be disabled, but any such notice does not modify the licensee's obligation to comply with paragraphs (c)(3)(i) and (ii) of this section.

(iv) *Notification to the Designated Correctional Facility Official.* Within two business days of receiving a qualifying request from a DCFO, a licensee must inform the DCFO whether the request has been granted or rejected.

(4) *Reversals.* A licensee may reverse a disabled wireless device if it determines that the wireless device was identified erroneously as contraband. The licensee must promptly inform the DCFO of the erroneously identified wireless device.

(i) *DCFO involvement.* Prior to reversing a disabling action, a wireless provider that determines that a device may have been erroneously identified as contraband may request that the DCFO review and confirm the information provided in a qualifying request pursuant to which the device was previously disabled. To trigger DCFO involvement, the wireless provider must provide the DCFO with:

(A) The date of the qualifying request;

(B) The identifying information provided for the device; and

(C) Any evidence supporting the wireless provider's belief that the device was erroneously identified.

(ii) *DCFO response.* Upon receipt of a request from a wireless provider, the DCFO should review the qualifying request and determine whether the device in question was erroneously identified and either confirm the validity of the identifying information contained in the qualifying request or acknowledge the error and direct the carrier to restore service to the device.

(iii) *Restoration of service.* In the event the DCFO directs the wireless provider to reverse the disabling, the wireless provider must, within two business days, restore service to the device and reverse any actions taken to prevent the device from accessing other wireless provider networks.

(iv) *Wireless provider action in absence of timely DCFO response.* In the event the DCFO does not respond to a request from a wireless provider for review of a qualifying request within two business days, the wireless provider may proceed with reversing the disabling action.

(v) *Notice of reversals.* The DCFO must provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices on a quarterly basis at the end of any quarter during which a device disabling was reversed.

(d) *Notification to Managed Access System (MAS) operators of wireless provider technical changes*—(1) *Notification requirements.* CMRS licensees leasing spectrum to MAS operators must provide 90 days' advance notice to MAS operators of the following network changes occurring within 15 miles of the correctional facility, unless parties modify notification arrangements through mutual agreement:

(i) Adding a new frequency band to service offerings;

(ii) Deploying a new air interface technology or changing an existing air interface technology; and/or

(iii) Adding, relocating, or removing a site.

(2) *Good faith negotiations.* CMRS licensee lessors and MAS operator lessees must negotiate in good faith to reach an agreement for notification for other types of network adjustments not covered by the notice requirement set

forth in paragraph (d)(1) of this section and for the parties' treatment of confidential information contained in notifications required pursuant to this section and/or negotiated between the parties.

(3) *Emergency network changes exception.* CMRS licensees leasing spectrum to managed access systems (MAS) operators are not required to provide 90 days' advance notice to MAS operators of network technical changes occurring within 15 miles of the correctional facility that are required due to emergency and disaster preparedness. CMRS licensees must provide notice of these technical changes immediately after the exigency.

[FR Doc. 2021–15748 Filed 8–12–21; 8:45 am]

BILLING CODE 6712–01–P